UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,251	03/30/2004	Satyajit Nath	2222.5500000	8159

26111 7590 11/26/2010

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2432	
MAIL DATE	**DELIVERY MODE**
11/26/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,251	NATH, SATYAJIT	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 September 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) *13-28 and 46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 29-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on 9/15/10.

2. Claims 1-46 are pending.

3. Claims 13-28 and 46 are withdrawn.

Response to Amendment

4. The 101 rejection of claims 29, 30 and 32-44 are withdrawn in view of the amendments to claims 29, 30 and 32-44.

5. The amendment to claims 38-44 overcome the 102(a) rejection as being anticipated by a conventional CD storing text data.

Response to Arguments

6. Applicant's argument that the prior art does not teach the new limitation "wherein the cryptographic key is a document retention key or a key encrypted with a document retention key, and wherein the cryptographic key is protected by a document access policy" (see pgs. 19-24 and 2-28 of Applicant's Remarks filed on 9/15/10) is moot in view of the new rejections.

7. In view of Applicant's traversal of the official notice taken in the rejections of claims 4-8 and 45, (see pgs. 24-26 of the Remarks filed on 9/15/10), the following evidence is provided to illustrate that such a teaching is common knowledge:

8. McKeehan et al. US 6,353,859 disclose an object-oriented apparatus and method for controlling accesses to objects in a distributed object environment. On col. 4, line 5-col. 5, line 30, McKeehan et al. disclose the invention with respect to a computing system. See fig. 1. In particular, McKeehan discloses:

> It is also important to point out that the presence of network interface 160 within computer system 100 means that computer system 100 may engage in cooperative processing with one or more other computer systems or workstations. Of course, this in turn means that the programs shown in main memory 120 need not necessarily all reside on computer system 100. For example, one or more portions of program 122 may reside on another system and engage in cooperative processing with one or more programs that reside on computer system 100. This cooperative processing could be accomplished through use of one of the well known client-server mechanisms such as remote procedure calls (RPC).

9. Jensen et al. US 6,185,612 disclose a secure distribution and use of network topology information. On col. 9, lines 4-58, Jensen et al. disclose:

> During a request making step 502, a path selector 206 or other requester makes a request for topology information 214. Suitable request formats are discussed in connection with FIG. 6. During a receiving step 504, the request is received by the manager 212. Suitable means for transmitting the request to the manager 212 are well known in the art, including network communication tools and techniques as well as interprocess communication tools and techniques such as remote procedure calls and shared memory. In many cases the requesting step 502 and the receiving step 504 will be performed on different network nodes, but the requester and the manager 212 may also run on the same node in some embodiments.

10. Wikipedia “Remote procedure call" disclose:

> RPC is an easy and popular paradigm for implementing the client-server model of distributed computing. An RPC is initiated by the caller (client) sending a request message to a remote system (the server) to execute a certain procedure using arguments supplied. A result message is returned to the caller.

Hence, in view of the documentary evidence, the basis of obviousness for the rejections of claims 4-8 and 45 are maintained.

Claim Rejections - 35 USC § 103

11. Claims 1-3 and 33-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merriam US 6,915,435 (hereinafter Merriam) in view of Pensak et al. US 6,289,450 (hereinafter Pensak et al.).

12. As per claims 1-3, Merriam discloses a method of electronic document retention, comprising:

a. assigning a document retention policy to the electronic document, the document retention policy being based on a future event that is unscheduled (col. 4:21-49, retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of);

b. cryptographically associating, using a cryptographic key, the document retention policy with the electronic document, wherein the cryptographic key is a document retention key or a key encrypted with a document retention key (4:12-31, document is encrypted using a public key, the corresponding private key is stored in a key repository, and key availability is dependent on the retention policy for the encrypted information set);

c. determining whether the future event has occurred; and cryptographically preventing access to the electronic document in accordance with the document retention policy based on the occurrence of the future event (4:60-6:44, when a condition is met, the decryption key is deleted by the retention manager, thereby preventing decryption of the encrypted information set);

d. the determining is performed periodically (fig. 3, retention policy is checked cyclically; periodic checking is de facto standard).

13. Merriam does not disclose that the cryptographic key is protected by a document access policy. Pensak et al. disclose an information security architecture whereby electronic documents can only be decrypted by authorized users. See Abstract. In particular, Pensak et al. disclose associating a portion of an encrypted document with a decryption key, and devising policies that restricts access to the decrypted document based on the group membership of the requestor. See col. 8:35-40; 9:4-14. Only after a user has been authorized to access a segment of a document is the user given access to the decryption key to decrypt the segment. See col. 8:35-38. Merriam as modified by Pensak et al. would suggest to one of ordinary skill in art to enable access to a decryption key for a user only if the user is authorized to access a secured electronic file. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Merriam such that the cryptographic key is protected by a document access policy. One would be motivated to do so to prevent a requestor from decrypting the encrypted content who does not have the proper permissions. The aforementioned cover the limitations of claims 1-3.

14. As per claims 33-37, Merriam discloses a file security system for restricting access to electronic files, said file security system comprising:

e. a processor; a memory having instructions stored thereon, that, in response to execution by the processor (see col. 8, line 7-col. 9, line 63), cause the processor to restrict access to electronic files (see col. 6, lines 50-64. file access requires the proper encryption/decryption key id), the instructions comprising:

f. Instructions for storing a plurality of cryptographic key pairs in a key store, each of the cryptographic key pairs including a public key and a private key, at least one of the cryptographic key pairs pertaining to a retention policy, wherein the cryptographic key pairs are document retention keys or keys encrypted with a document retention key (fig. 1, reference no. 114 “key repository”, col. 4:12-20, public/private keys; public keys are used to encrypt the information sets), the retention policy being dependent on a future event (4:36-49, retention policies are based on conditions); and

g. Instructions for determining whether the private key of the at least one of the cryptographic key pairs pertaining to the retention policy is permitted to be provided to a requestor based on whether the future event has occurred, wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the retention policy to access a secured electronic file, and wherein the secured electronic file was previously secured using the public key of

the at least one of the cryptographic key pairs pertaining to the retention policy, and at the time the electronic file was so secured, the future event was unscheduled (fig. 1, reference no. 116 “retention manager”; 4:28-49, retention manager manages the retention of “information sets” based on a time period, condition policy, classification-based policy or any combinations there of; 5:11-55, encrypting the received information set with a cryptographic key);

h. wherein the instructions for determining comprise instructions for preventing the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from being provided to the requestor after a predetermined retention period following the occurrence of the future event (5:56-6:13, 6:27-44, the decryption key is deleted if the encrypted information set is to be purged based on the retention policy);

i. wherein the requestor is a client module that operatively connects to said access manager over a network (fig. 1, reference no. 106, “information sink”, 3:32-49);

j. wherein said file security system further comprises: at least one client module, configured to assist in selecting the retention policy and secure the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy so as to cryptographically impose the retention policy (4:33-49, 6:14-26, retention manager operates by implementing a predetermined information retention policy; see generally, figure 6 and col. 8:39-44);

k. wherein said file security system further comprises: at least one client module, said client module assisting with unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertains to the retention policy from said key store if permitted by said access manager, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertains to the retention policy (7:20-8:7, information sink acquires decryption key from the information manager).

15. Merriam does not disclose that the cryptographic key is protected by a document access policy. Pensak et al. disclose an information security architecture whereby electronic documents can only be decrypted by authorized users. See Abstract. In particular, Pensak et al. disclose associating a portion of an encrypted document with a decryption key, and devising policies that restricts access to the decrypted document based on the group membership of the requestor. See col. 8:35-40; 9:4-14. Only after a user has been authorized to access a segment of a document is the user given access to the decryption key to decrypt the segment. See col. 8:35-38. Merriam as modified by Pensak et al. would suggest to one of ordinary skill in art to enable access to a decryption key for a user only if the user is authorized to access a secured electronic file. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Merriam such that the cryptographic key is protected by a document access policy. One would be motivated

to do so to prevent a requestor from decrypting the encrypted content who does not have the proper permissions. The aforementioned cover the limitations of claims 33-37.

16. As per claims 38-41, Merriam discloses a non-transitory computer readable medium having computer-executable instructions stored thereon for providing data retention for electronic data, the computer-executable instructions comprising:

l. instructions to assign computer program code for assigning a data retention policy to the electronic data, the data retention policy being based on a future event that is unscheduled (col. 4:21-49, retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of);

m. instructions to cryptographically associate, using a cryptographic key, computer program code for cryptographically associating the data retention policy with the electronic data, wherein the cryptographic key is a document retention key or a key encrypted with a document retention key (4:12-31, document is encrypted using a public key, the corresponding private key is stored in a key repository, and key availability is dependent on the retention policy for the encrypted information set);

n. wherein said computer readable medium the instructions further comprise: instructions to cryptographically prevent computer program code for cryptographically preventing access to the electronic data in accordance with the data retention policy based on the occurrence of the future event (4:21-49, 6:27-

44, decryption keys are deleted when corresponding information set is to be purged under the retention policy);

o. wherein the electronic data is an electronic file; wherein the electronic data is an electronic document (3:20-31, information set broadly refers to any digital data including files).

17. Merriam does not disclose that the cryptographic key is protected by a document access policy. Pensak et al. disclose an information security architecture whereby electronic documents can only be decrypted by authorized users. See Abstract. In particular, Pensak et al. disclose associating a portion of an encrypted document with a decryption key, and devising policies that restricts access to the decrypted document based on the group membership of the requestor. See col. 8:35-40; 9:4-14. Only after a user has been authorized to access a segment of a document is the user given access to the decryption key to decrypt the segment. See col. 8:35-38. Merriam as modified by Pensak et al. would suggest to one of ordinary skill in art to enable access to a decryption key for a user only if the user is authorized to access a secured electronic file. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Merriam such that the cryptographic key is protected by a document access policy. One would be motivated to do so to prevent a requestor from decrypting the encrypted content who does not have the proper permissions. The aforementioned cover the limitations of claims 38-41.

18. Claims 4-8 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merriam in view of Pensak et al. Reference is also made to McKeehan et al. US 6,353,859, Jensen et al. US 6,185,612 and Wikipedia “Remote procedure call" as evidence to support the official notice that it is common knowledge in the art to distribute process handling over a network.

19. As per claims 4-8 and 45, the rejection of claim 2 under 35 USC 102(e) as being anticipated by Merriam is incorporated herein. Furthermore, Merriam discloses the retention manager implements a retention policy, whereby the manager determines if a stored information set should be retained based on a condition. Although Merriam does not disclose a network accessible resource whereby the resource determines if a condition has occurred based on a future event description transmitted over the Internet, it is notoriously well known in the art to distribute process handling to remote systems. This concept is known as distributive processing. Distributive processing utilizes a collection of computers that communicate over a network to perform different processing roles within a larger framework. One means by which remote computers perform such tasks is the use of remote procedure calls (RPC). Distributive processing enables the workload to be segregated based on a separation of concerns. Official notice of this teaching is taken.

In view of Applicant’s traversal of this official notice (see pgs. 24-26 of Applicant’s Remarks filed on 9/15/10) the following evidence is provided to illustrate that such teaching is common knowledge:

20. McKeehan et al. US 6,353,859 disclose an object-oriented apparatus and method for controlling acesses to objects in a distributed object environment. On col. 4, line 5-col. 5, line 30, McKeehan et al. disclose the invention with respect to a computing system. See fig. 1. In particular, McKeehan discloses:

> It is also important to point out that the presence of network interface 160 within computer system 100 means that computer system 100 may engage in cooperative processing with one or more other computer systems or workstations. Of course, this in turn means that the programs shown in main memory 120 need not necessarily all reside on computer system 100. For example, one or more portions of program 122 may reside on another system and engage in cooperative processing with one or more programs that reside on computer system 100. This cooperative processing could be accomplished through use of one of the well known client-server mechanisms such as remote procedure calls(RPC).

21. Jensen et al. US 6,185,612 disclose a secure distribution and use of network topology information. On col. 9, lines 4-58, Jensen et al. disclose:

> During a request making step 502, a path selector 206 or other requester makes a request for topology information 214. Suitable request formats are discussed in connection with FIG. 6. During a receiving step 504, the request is received by the manager 212. Suitable means for transmitting the request to the manager 212 are well known in the art, including network communication tools and techniques as well as interprocess communication tools and techniques such as remote procedure calls and shared memory. In many cases the requesting step 502 and the receiving step 504 will be performed on different network nodes, but the requester and the manager 212 may also run on the same node in some embodiments.

22. Wikipedia “Remote procedure call" disclose:

> RPC is an easy and popular paradigm for implementing the client-server model of distributed computing. An RPC is initiated by the caller (client) sending a request message to a remote system (the server) to execute a certain procedure using arguments supplied. A result message is returned to the caller.

23. It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the determining comprises interacting with a network accessible resource, wherein the network accessible resource is one or more of a server, an application, or a system; wherein the determining comprises interacting with a web accessible resource, wherein the web accessible resource is one or more of a web server, an application, or an external system; the determining comprises: supplying a future event description of the future event to the web accessible resource; and determining, at the web accessible resource, whether the future event has occurred; wherein said supplying is achieved by a universal resource locator associated with the future event description; and wherein the determining comprises: supplying the future event description to a contract management system; determining, at the contract management system, whether the future event has occurred; and supplying a future event description of the future event to the network accessible resource; and determining, at the network accessible resource, whether the future event has occurred. One would be motivated to do so to enable the workload to be segregated based on a separation of concerns. The aforementioned cover the limitations of claims 4-8 and 45.

24. Claims 9-12, 29-32 and 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merriam in view of Pensak et al. and Todd et al. US 7,249,251 (hereinafter Todd)

25. As per claims 9-12, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Merriam in view of Pensak et al. is incorporated herein. In addition, Merriam discloses deactivating the cryptographic key in response to determining that a document retention period has expired, thereby preventing further access to the electronic document. See Merriam, col. 4:21-49, 6:27-44 (decryption keys are deleted when corresponding information set is to be purged under the retention policy; retention policies can be based on retention periods). Furthermore, as noted above, on col. 4:21-49, Merriam discloses that the retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of. However, Merriam does not expressly disclose the document retention policy specifies a document retention period based on the future event; wherein the document retention policy specifies a document retention period that expires a predetermined period of time after the occurrence of the future event; and permitting the deactivating step to be overridden so that the electronic document can remain accessible even after the document retention period. Todd discloses a method and apparatus for secure modification of a retention period for data in a storage system, where data is retained for a specified period after a future event. See col. 6:53-61 (x-rays are retained 2 years after the death of patient). Modifications can be made to either shorten or extend the original retention period. See col. 7:7-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the document retention policy specifies a document retention period based on the future event; wherein the document retention policy specifies a document retention period that

expires a predetermined period of time after the occurrence of the future event; and permitting the deactivating step to be overridden so that the electronic document can remain accessible even after the document retention period. One would be motivated to do so to enable retention period modification as taught by Todd. The aforementioned cover the limitations of claims 9-12.

26. As per claims 29-32, Merriam discloses a computer-implemented method for distributing cryptographic keys used in a file security system, said method comprising:

p. Receiving, at a computing device, a request for a document retention key that is necessary to gain access to a cryptographically secured electronic document (7:20-8:7, information sink acquires decryption key from the information manager);

q. Identifying, at a computing device, a document retention period associated with the document retention key; determining, by the computing device, whether the document retention period associated with the document retention key has been exceeded; and refusing to distribute the document retention key in response to determining that the document retention period for the electronic document has been exceeded (col. 4:21-49, 6:27-44, decryption keys are deleted when corresponding information set is to be purged under the retention policy; col. 4:21-49, the retention manager manages the retention of “information sets” based on a time period, condition policy, classification-based policy or any combinations there of);

r. wherein said computing device is a server, and wherein the request for the document retention key is from a client module that is connectable to the server via a network (3:32-48, information system can be a server and information sink would be a client).

27. Merriam does not disclose that the cryptographic key is protected by a document access policy. Pensak et al. disclose an information security architecture whereby electronic documents can only be decrypted by authorized users. See Abstract. In particular, Pensak et al. disclose associating a portion of an encrypted document with a decryption key, and devising policies that restricts access to the decrypted document based on the group membership of the requestor. See col. 8:35-40; 9:4-14. Only after a user has been authorized to access a segment of a document is the user given access to the decryption key to decrypt the segment. See col. 8:35-38. Merriam as modified by Pensak et al. would suggest to one of ordinary skill in art to enable access to a decryption key for a user only if the user is authorized to access a secured electronic file. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Merriam such that the cryptographic key is protected by a document access policy. One would be motivated to do so to prevent a requestor from decrypting the encrypted content who does not have the proper permissions.

28. Finally, Merriam does not disclose the document retention period being dependent on a future event that was unscheduled when the document retention period was associated with the electronic document; wherein the document retention period is

a predetermined period of time after the occurrence of the future event; and wherein the document retention period can be extended to permit extended access to the electronic document. Todd discloses a method and apparatus for secure modification of a retention period for data in a storage system, where data is retained for a specified period after a future event. See col. 6:53-61 (x-rays are retained 2 years after the death of patient). Modifications can be made to either shorten or extend the original retention period. See col. 7:7-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the document retention period to be dependent on a future event that was unscheduled when the document retention period was associated with the electronic document; wherein the document retention period is a predetermined period of time after the occurrence of the future event; and wherein the document retention period can be extended to permit extended access to the electronic document. One would be motivated to do so to enable retention period modification as taught by Todd. The aforementioned cover the limitations of claims 29-32.

29. As per claims 42-44, the rejection of claim 38 under 35 USC 103(a) as being unpatentable over Merriam in view of Pensak et al. is incorporated herein. In addition, Merriam discloses instructions to deactivate computer program code for deactivating the cryptographic key in response to determining that the data retention period has expired, thereby preventing further access to the electronic data; and the instructions further comprises: instructions to determine computer program code for determining whether the data retention period has expired. See Merriam col. 4:21-49, 6:27-44 (decryption

keys are deleted when corresponding information set is to be purged under the retention policy). Furthermore, as noted above, on col. 4:21-49, Merriam discloses that the retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of. However, Merriam does not expressly disclose the data retention policy specifies a data retention period based on the future event; wherein: the data retention policy specifies a data retention period that expires a predetermined period of time after the occurrence of the future event; and wherein the instructions further comprises: instructions to permit deactivation of the cryptographic key computer program code for permitting said computer program code for deactivating to be overridden so that the electronic data can remain accessible even after the data retention period. Todd discloses a method and apparatus for secure modification of a retention period for data in a storage system, where data is retained for a specified period after a future event. See col. 6:53-61 (x-rays are retained 2 years after the death of patient). Modifications can be made to either shorten or extend the original retention period. See col. 7:7-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the data retention policy to specify a data retention period based on the future event; wherein: the data retention policy specify a data retention period that expires a predetermined period of time after the occurrence of the future event; and wherein the instructions further comprises: instructions to permit deactivation of the cryptographic key computer program code for permitting said computer program code for deactivating to be overridden so that the electronic data can remain accessible even after the data

retention period. One would be motivated to do so to enable retention period modification as taught by Todd. The aforementioned cover the limitations of claims 42-44.

Conclusion

30. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432